Amendments to the Claims

1. (canceled)

2. (currently amended) The method of claim 46 [[1]], wherein ~~said~~ the network security protocol is SSL (v3).

3. (currently amended) The method of claim 46 [[1]], wherein ~~said~~ the network security protocol is TLS.

4.-27. (canceled)

28. (currently amended) The method of claim 46 [[1]] comprising ~~packing~~ aligning the received ~~non-pre-padded network security protocol~~ set of header data for the first packet.

29. (currently amended) The method of claim 28 [[26]] comprising storing the aligned ~~network security protocol~~ set of header data for the first packet in a FIFO to accumulate a predefined amount of data before commencing the authentication operations ~~and the at least one of encryption operations and decryption operations~~.

30. (previously presented) The method of claim 29 wherein the predefined amount of data comprises 512 bits.

31. (canceled).

32. (currently amended) The method of claim 28 [[31]] where the ~~at least a portion of the~~ aligned ~~network security protocol~~ set of header data for the first packet

comprises Content Type, Length and Data that is aligned into rows of data where each row of data contains a single type of data.

33. (currently amended) The method of claim 31 comprising aligning, for encryption operations, the set of data in the payload data for the first packet ~~at least a portion of the received non-pre-padded network security protocol data and the authenticated at least a portion of the aligned network security protocol data~~ to provide the aligned ~~network security protocol~~ data for the encryption operations.

34. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises removing non-valid data.

35. (previously presented) The method of claim 33 wherein aligning, for encryption operations, comprises adding padding.

36. (currently amended) The method of claim 33 [[26]] comprising storing the aligned set of data in the payload data for the first packet ~~network security protocol data~~ for the encryption operations in a FIFO to accumulate a predefined amount of data before commencing the encryption operations.

37.-43. (canceled)

44. (currently amended) The method of claim 46 [[1]] wherein:

the authentication operations are performed by an authentication component of the chip;

the encryption operations are performed by an encryption component of the chip; and

authentication data generated by the authentication component is passed to the encryption component and aligned by the encryption component.

45. (currently amended) The method of claim 46 [[1]] wherein:

the authentication operations are performed by an authentication component of the chip;

the encryption operations are performed by an encryption component of the chip; and

decrypted data generated by the encryption component is passed to the authentication component and aligned by the authentication component.

46. (new) A method for accelerating cryptographic processing of a plurality of data packets according to a network security protocol, comprising:

receiving, in a chip, header data and payload for a first packet from an off-chip processor;

performing authentication operations on a set of header data and the payload data for the first packet to generate an authentication code;

performing encryption operations on a set of data in the payload data for the first packet, wherein the encryption operations on the set of payload data for the first packet is performed in parallel with the authentication operations for the first packet;

receiving, in the chip, header data and payload data for a second packet;

performing encryption operations on any remaining payload data for the first packet and the authentication code for the first packet;

performing authentication operations on a set of header data and the payload data for the second packet, wherein the authentication operations on the set of header data and payload data for the second packet is performed simultaneously with the encryption operations on the remaining payload data and authentication code for the first packet; and

passing the cryptographically processed first packet from the chip to the off-chip processor,

wherein the authentication and encryption operations for the first packet are performed within the chip in a single pass.